IN THE CLAIMS

1. (Currently Amended) A method to detect unauthorized reconnaissance or scanning of a computer network comprising the acts of:

~~(a)~~ monitoring communications within the network;

~~(b)~~ detecting a predefined ~~sequence~~ sequential triplet of TCP/IP protocol set packets flowing within said communications, comprising the steps of:

observing an initial SYN packet originating from a source address;

detecting a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet; and

detecting a last sequential RST packet originating from the source address in response to the SYN/ACK packet; and

~~(c)~~ issuing an alert indicating unauthorized scanning if the predefined sequence of packets ~~is detected~~ are each relevant to the source address.

2. (Original) The method of claim 1 wherein the monitoring is done within a selected network device.

3. (Currently Amended) The method of claim 1 or claim 2 wherein the detecting act further includes the acts of:

providing a histogram in which states of the predefined sequence of packets are maintained; and

dynamically updating said histogram as selected ones of the predefined sequence of ~~packet~~ packets is detected.

4. (Original) The method of claim 3 wherein the histogram includes a table partitioned into a first field in which source addresses of network devices are kept; and a second field, concatenated to the first field, in which a code representing states in which packets in the predefined sequence of packets are detected.

Claims 5-7. (Cancelled)

8. (Currently Amended) The method of claim 1 wherein the issuing act further includes the ~~acts~~ act of sending a message to an administrator.

9. (Original) The method of claim 1 wherein the issuing act further includes the act of blocking future packets from network computers having predefined characteristics.

10. (Original) The method of claim 1 wherein the issuing act further includes the act of rate-limiting flows of packets from network devices having predefined characteristics.

11. (Currently Amended) An intrusion detection system, ~~including~~comprising:

a memory device comprising a table containing at least one characteristic identifying network devices and a set of state code corresponding to a sequence in which a predefined ~~set of~~ sequential triplet of TCP/IP protocol packets are observed, the triplet comprising:

an initial SYN packet originating from a source address;

a next sequential SYN/ACK packet issued from a target device address in response to the SYN packet; and

a last sequential RST packet originating from the first source address in response to the SYN/ACK packet; and

a processor means in communication with the memory device, ~~a controller operable~~ wherein the processor means is configured to examine received packets[,] flowing within computer network communications for the triplet;

wherein the processor means is further configured to access the memory device table and ~~to~~ adjust the state code in response to observing the triplet; and

wherein the processor means is further configured to generate an alert if one of the set of state code reaches a predefined value.

12. (Currently Amended) The intrusion detection system of claim 11 wherein the at least one characteristic includes a ~~Source Address~~ source address.

13. (Currently Amended) The intrusion detection system of claim 11 wherein the set of state code corresponding to the sequence triplet of predefined packets includes 00 representing a default, 01 representing ~~a first of the sequence of predefined packets~~ the SYN packet, 10 representing ~~a second of the sequence of predefined packets~~ the SYN/ACK packet and 11 representing ~~last of the sequence of predefined packets~~ the RST packet.

Claims 14-15. (Cancelled)

16. (Currently Amended) The intrusion detection system of claim 11 wherein the ~~controller~~ processor means includes a programmed general purpose computer.

17. (Currently Amended) The intrusion detection system of claim 11 wherein the ~~controller~~ processor means includes a programmed specialized computer.

18. (Original) The intrusion detection system of claim 17 wherein the specialized computer includes a network processor.

19. (Original) The intrusion detection system of claim 17 wherein the predefined value includes "11".

20. (Currently Amended) A program product including:

_____a computer-readable medium; and

_____a computer program recorded on said medium, said computer program including a first set of instructions that ~~examine packets to detect a predefined sequence of packets;~~

~~and a second set of instructions that generate an alert if the predefined sequence of packets are detected~~, when executed on a computer, causes the computer to:

monitor communications within the network;

detect a predefined sequential triplet of TCP/IP protocol packets flowing within said communications, the triplet comprising an initial SYN packet originating from a source address, a next sequential SYN/ACK packet issued by a target device in response to the SYN packet; and a last sequential RST packet originating from the source address in response to the SYN/ACK packet; and

issue an alert indicating unauthorized scanning if the triplet packets are each relevant to the source address.

21. (Currently Amended) The program product of claim 20 further including a third set of instructions which, when executed on the computer, causes the computer to ~~responsive to the alert to~~ generate a message notifying an operator of an occurrence of an event responsive to the alert.

22. (Currently Amended) The program product of claim 21 wherein the event indicates unauthorized scanning of a device comprising the computer executing said program product.

Claim 23-24. (Cancelled).

25. (Currently Amended) A method to deploy an intrusion detection system on a network device including acts of:

providing an algorithm to detect a predefined ~~set~~ sequential triplet of TCP/IP protocol packets; and

generating an alert if the predefined ~~set~~ triplet of packets is detected and the triplet packets are each relevant to a source address;

wherein the triplet comprises an initial SYN packet originating from the source address, a next sequential SYN/ACK packet issuing from a target device address in

response to the SYN packet, and a last sequential RST packet originating from the source address in response to the SYN/ACK packet.

26. (Currently Amended) The method of claim 25 further including the act of providing a table to record at least one characteristic to identify network devices and state code corresponding to a sequence in which the predefined ~~set~~ sequential triplet of packets are received.

Claim 27-29. (Cancelled).

30. (Currently Amended) A method to protect devices from malicious attacks launched on a computer network including the acts of:

providing on a device to be protected a software program that monitors packets; and

issuing an alert if a predefined sequential triplet ~~set~~ of TCP/IP protocol packets are detected and the triplet packets are each relevant to a source address;

wherein the triplet comprises an initial SYN packet originating from the source address, a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet, and a last sequential RST packet originating from the source address in response to the SYN/ACK packet.

Claims 31-33. (Cancelled).

34. (Original) The method of claim 30 wherein the software program includes a table containing codes whose values represent detection of one of the predefined set of packets.

35. (Currently Amended) The method of claim 34 wherein the table further includes at least one source ~~Address (SA)~~address associated with at least one of the codes.